October 2009 - Standards Implementation Guidance: PRODUCT GUIDANCE			
Functionality	**Standards**	**Implementation Guidance (2011-2015)**	**Basic Definition**
Access Control	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(a) Access Control (HIPAA)	HIPAA Security Rule	The HIPAA Security Rule requires security mechanisms for controlling entities' access to protected resources.
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP 800-111 - Guide to Storage Encryption Technologies for End User Devices	This document helps organizations understand storage encryption technologies for end user devices and in planning, implementing, and maintaining storage encryption solutions.
	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/SC108 -- Access Control (Using any implementation of RBAC that supports permissions from the HL7 permissions catalog)	The Access Control service provides the mechanism for security authorizations which control the enforcement of security policies.
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/SC108	
	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141	HITSP/SC108	
	OASIS WS-Trust Version 1.3, March 2007	HITSP/SC108	

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
Audit	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(b) Audit Controls (HIPAA)	HIPAA Security Rule	The HIPAA Security Rule requires audit controls to record information about activities that occur, when they occur, and the users involved.
	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	HITSP/SC109 -- Security Audit	The Security Audit Service Collaboration describes the mechanism to record security relevant events in support of policy, regulation, or risk analysis.
Authentication	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Person or Entity Authentication (HIPAA)	NIST SP 800-63-1 - Electronic Authentication Guideline	The HIPAA Security Rule requires security mechanisms for authenticating the user identity asserted.
	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)	HITSP/C19 - Entity Identity Assertion	The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided.
Consent Management	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)		The HIPAA Privacy Rule sets for conditions under which consumers' consent is a precondition of specific types of accesses and uses of their individual protected health information (PHI).
	HITSP/CAP143 Manage Consumer Preference and Consents	HITSP/CAP143 -- Manage Consumer Preferences and Consents	This capability addresses management of consumer preferences and consents as an acknowledgement of a privacy policy. This capability is used to capture a patient or consumer agreement to one or more privacy policies; where examples of a privacy policy may represent a consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial. This capability also supports the recording of changes to prior privacy policies such as when a patient changes their level of participation or requests that data no-longer be made available because they have left the region.
	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile	HITSP/CAP143	
	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/CAP143	

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
Consumer EHR	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)	HIPAA Privacy Rule	The HIPAA Privacy Rule requires covered entities to provide consumers copies of their individual electronic health record at their request.
	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	This capability addresses interoperability requirements that support the communication of a set of unstructured health data related to a patient in a context set by the source of the document who is attesting to its content.
	HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)	HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)	This capability addresses interoperability requirements that support the communication of structured health data related to a patient in a context set by the source of the document who is attesting to its content. Several document content subsets, structured according to the HL7 CDA standard, are supported by this capability. The following are examples of the type of structured data that may be used: 1. Continuity of Care Document (CCD) 2. Emergency Department Encounter Summary 3. Discharge Summary (In-patient encounter and/or episodes of care) 4. Referral Summary Ambulatory (encounter and/or episodes of care) 5. Consultation Notes 6. History and Physical 7. Personal Health Device Monitoring Document 8. Healthcare Associated Infection (HAI) Report Document Document creators shall support a number of the HITSP specified coded terminologies as defined by specific content subsets specified in this capability.

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
HIPAA Deidentification	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(a-b) Deidentification of protected health information (HIPAA)	HIPAA Privacy Rule	The HIPAA Privacy Rule defines two methods for de-identifying protected health information to enable it to be used for purposes other than treatment, payment, and healthcare operations. In addition, it sets forth requirements for enabling a covered entity to implement a mechanism for re-associating de-identified information with the individual under certain circumstances.
	46 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(c) Reidentification (HIPAA)	HIPAA Privacy Rule	
	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization)	HITSP/C25 - Anonymize (for Biosurveillance and Quality)	The Anonymize Component provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery.
	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization)	HITSP/T24 -- Pseudonymize HITSP/C87 - Anonymize Public Health Case Reporting Data Component HITSP/C88 - Anonymize Immunizations and Response Mgmt Data	T24 -The Pseudonymize Transaction describes a framework for including Pseudonymization Services where the use of “dummy” or pseudo references to specific patients or providers is requred. C87 and C88 describe methods for anonymizing protected health information for reporting to public health agencies.

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
Data Integrity	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(c) Integrity (HIPAA)	HITSP/SC112 -- Healthcare Document Management	The Healthcare Document Management Service Collaboration provides the ability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1).	HITSP/C26 -- Nonrepudiation of Origin	The Nonrepudiation of Origin Component provides the mechanisms to support Nonrepudiation of Origin, which refers to both the proof of the integrity and origin of documents in a high-assurance manner, which can be verified by any party. This Component does not provide Nonrepudiation of Receipt.
	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	HITSP/C26	
	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	HITSP/C26	
	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	HITSP/C26	
	ISO/TS-17090, Health Informatics, Public Key Infrastructure	HITSP/C26	
Transmission Security	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Transmission Security (HIPAA)	HIPAA Security Rule	The HIPAA Security Rule sets forth standards and implementation specifications for security protected health information transmitted over vulnerability transmission media.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1).	HITSP/T17 -- Secure Communications Channel	The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties.
	FIPS 197, Advanced Encryption Standard, Nov 2001	HITSP/T17	
	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546	HITSP/T17	
	IETF Cryptographic Message Syntax (CMS), RFC-2630, -3852	HITSP/T17	

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	HITSP/T16 -- Consistent Time	The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks.
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	HITSP/T16	
	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile	HITSP/T16	
Document Exchange	HITSP/SC112 - Healthcare Document Management	HITSP/SC112 -- Healthcare Document Management	The Healthcare Document Management Service Collaboration provides the ability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community (made up of potentially diverse Health Information Exchanges).
	IHE ITI-TF Cross Enterprise Document Reliable Interchange (XDR) Integration Profile	HITSP/SC112	
	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile	HITSP/SC112	
	IHE ITI-TF Revision 5.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/SC112	
	OASIS/ebXML Registry Information Model v3.0	HITSP/SC112	
	OASIS/ebXML Registry Services (ebRS) Specifications v3.0	HITSP/SC112	
	IHE ITI-TF Revision 5.0 or later, Cross Community Access (XCA) Profile	HITSP/SC112	
	IHE ITI-TF Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile	HITSP/SC112	
	HL7 V3 Confidentiality Codes value set	HITSP/SC112	

Functionality	Standards	Implementation Guidance (2011-2015)	Basic Definition
Service Access	OASIS Simple Object Access Protocol (SOAP) Version 1.2	IHE ITI-TF Vol 2: Appendix V (Web Services for IHE Transactions)	Appendix V of the IHE ITI Technical Framework provides guidelines for specifying the use of SOAP-based Web Services as the messaging infrastructure and transport mechanism for IHE transactions.
	OASIS Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006	IHE ITI-TF Vol 2: Appendix V (Web Services for IHE Transactions)	
Domain Name Service	IETF: RFC-2181, -2219, -2782. Domain Name Service (DNS) services	HITSP/T64 -- Personnel White Pages	The Identify Communication Recipients Transaction is intended to serve the purpose of identification of communication recipients and the subsequent purpose of delivery of alerts and bi-directional communications (e.g., public health agencies notifying a specific group of service providers about an event.) The method and criteria by which individuals are added to a directory is a policy decision, which is out of scope for this construct. It uses the Integrating the Healthcare Enterprise (IHE) Personnel White Pages profile which provides access to basic directory information for identifying one or more recipients.
Directory Access	IETF: RFC-2251, -2252, -2253. Lightweight Directory Access Protocol (LDAP)	HITSP/T64 -- Personnel White Pages -- any directory schema is allowed	The HITSP T64 Identify Communication Recipients Transaction construct is intended to serve the purpose of identification of communication recipients and the subsequent purpose of delivery of alerts and bi-directional communications (e.g., public health agencies notifying a specific group of service providers about an event.) This construct uses the Integrating the Healthcare Enterprise (IHE) Personnel White Pages (PWP) profile which provides access to basic directory information for identifying one or more recipients.
	IHE ITI-TF Revision 4.0 or later, Personnel White Pages (PWP)	HITSP/T64	
	RFC 1766 Tags for the Identification of Languages	HITSP/T64	